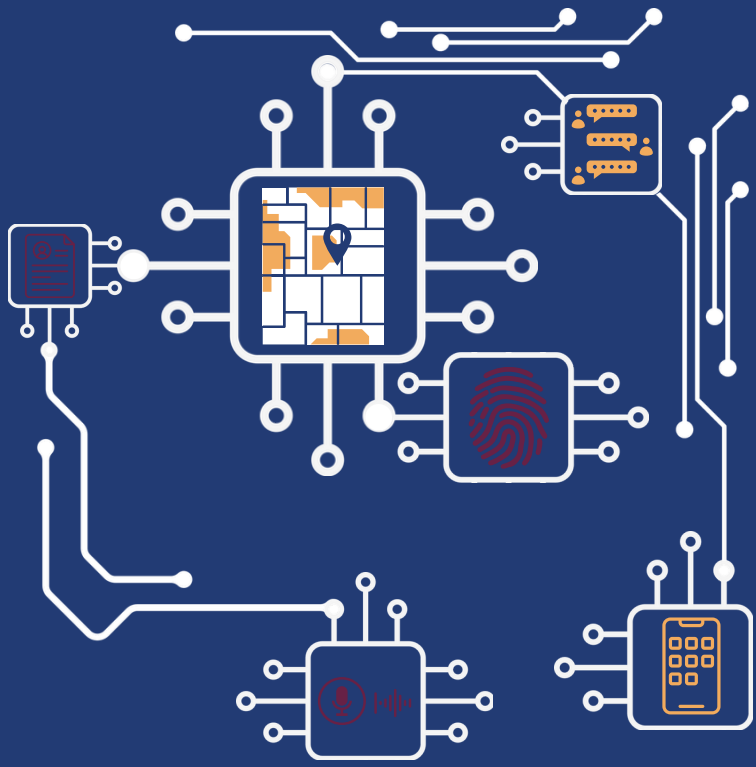
OSCE
the representative on freedom of the media

A HIGHER STANDARD FOR MEDIA FREEDOM AND JOURNALISTIC PROTECTION AGAINST ARBITRARY OR UNLAWFUL SURVEILLANCE



Copyright: Creative Commons Attribution-Non Commercial-Share Alike 4.0 International (CC BY-NC-SA 4.0)

ISBN: 978-92-9234-695-9

© 2026 Office of the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media

Wallnerstrasse 6
1010 Vienna, Austria
Phone.: +43-1 514 36 68 00
E-mail: pm-fom@osce.org
https://www.osce.org/fom

This publication was produced as part of the project "Healthy Online Information Spaces – SAIFE Renewed" by the Office of the OSCE Representative on Freedom of the Media (OSCE RFoM) in collaboration with the Centre for Democracy and Technology Europe (CDT Europe). It consists of a Policy Brief and 10 Action Points.

Policy Brief
Authors: Lisa Beatrice Ferrari and Rand Hammoud, CDT Europe
Editor: Julia Haas, OSCE RFoM

The views expressed in this publication are those of the authors and do not necessarily represent the official position of the OSCE or its participating States.

Action Points
The Action Points are guidance by the OSCE RFoM. They were developed by Julia Haas on the basis of an expert workshop (Vienna, 22 September 2026), consultations, and written contributions, some of them anonymous. Participation in this process does not imply that every Action Point reflects the full position of each contributing organization or expert.

Acknowledgments
The OSCE RFoM thanks the following organizations for their contributions: Article 19, Centre for Democracy and Technology Europe, Committee to Protect Journalists, Daktilo 1984, European Digital Rights, European Federation of Journalists, International Federation of Journalists, Inside Story, IrpiMedia, King's College London, Media Defence, MediaNet International Centre for Journalism, Panoptykon Foundation, Privacy International, Reporters Without Borders, RESIDENT.NGO, SHARE Foundation; as well as OSCE colleagues, including from the Action against Terrorism Unit and Strategic Police Matters Unit. Additional experts, including journalists in exile, were also consulted and involved in the process.

Project Assistant
Claire Haering, OSCE RFoM

Design & Layout
Benjamin Fischer, OSCE RFoM





TABLE OF CONTENTS

Preface	5
Policy Brief	8
Introduction	9
Commitments and Legal Background	18
Surveillance Threshold	24
Authorization	28
Oversight	31
Redress: Notification, Support, Effective Remedies	33
Third-Party and Transnational Surveillance	37
Procurement, Export, and Investment	39
Technological Safeguards	44
Conclusion	48
10 Action Points	51

A HIGHER STANDARD FOR MEDIA FREEDOM AND JOURNALISTIC PROTECTION AGAINST ARBITRARY OR UNLAWFUL SURVEILLANCE

Democratic societies depend on journalists and other media actors being able to work freely, independently, and safely, without interference or fear. Surveillance threatens this essential freedom, undermining their ability to report in the public interest, protect confidential sources, and hold power to account.

This document aims to support the participating States of the Organization for Security and Co-operation Europe (OSCE) in operationalizing their commitment under OSCE Ministerial Council Decision No. 3/18 on the Safety of Journalists to refrain from arbitrary or unlawful surveillance of journalists or interference with their use of encryption and anonymity technology. It provides 10 action points for State institutions to prevent undue surveillance of journalists and their sources. "Undue surveillance" is used here for surveillance that is arbitrary or unlawful, or that otherwise undermines the democratic role and public interest function of the media. The action points refer to all persons performing a journalistic function, in line with the functional approach of the UN Human Rights Committee General Comment No. 34, and to surveillance that affects media freedom whether or not it targets a journalist directly.

While international human rights law does not prohibit surveillance outright, it permits surveillance only where it is prescribed by law, pursues a legitimate aim, and is necessary and proportionate, with non-discrimination and adequate procedural safeguards. States should refrain from subjecting journalists to surveillance, except in exceptional circumstances involving a clear and immediate threat to public security. Any measure that

risks interfering with journalistic activities, exposing journalistic sources, or otherwise undermining media freedom must meet a particularly high threshold of justification and be subject to stringent legal and procedural safeguards, as set out below.

This publication first presents the 10 action points to prevent undue surveillance of journalists and their sources as an overview, followed by a policy brief providing the background, complexities and foundations of surveillance of journalists requiring stronger protective frameworks (pages 8–50). It concludes with the detailed action points and concrete measures on operationalization (pages 51-62).

10 ACTION POINTS

1. PRESERVE privacy, online anonymity and secure communications infrastructures to safeguard freedom of expression and media freedom
2. PREVENT undue surveillance through a robust legal framework
3. PRIORITIZE independent, individualized, narrowly scoped authorization
4. PERFORM independent oversight
5. PROVIDE accountability and redress through notifications, investigations, and remedies
6. PUBLISH information and guarantee transparency
7. PROCURE and invest in accordance with human rights
8. PROTECT journalists and their sources across borders through export control
9. PRECLUDE proliferation through market regulation
10. PROMOTE human rights through multi-stakeholder partnerships and support

The action points build on international human rights law and OSCE commitments, in particular the right to privacy (International Covenant on Civil and Political Rights [ICCPR] Art. 17; Universal Declaration of Human Rights [UDHR] Art. 12), freedom of expression and media freedom (ICCPR Art. 19; UDHR Art. 19), and the right to an effective remedy (ICCPR Art. 2(3)), as well as the UN Guiding Principles on Business and Human Rights. They also draw on the interpretation of these rights in UN Human Rights Committee General Comments Nos. 16 and 34, UN General Assembly and Human Rights Council resolutions on the right to privacy in the digital age and the safety of journalists, and reports by the Office of the United Nations High Commissioner for Human Rights (OHCHR) and UN Special Rapporteurs. They are also informed by the case law of the European Court of Human Rights, Council of Europe Recommendation CM/Rec(2016)4, and other relevant regional and national legislation as well as international frameworks such as the Pall Mall Process. The publication expands on Communiqué No. 1/2023 by the OSCE Representative on Freedom of the Media.

The action points are addressed to State institutions, such as legislators, authorizing and oversight bodies, law enforcement and intelligence agencies, as well as procurement and export-licensing authorities. A robust legal framework is the basis for implementing the action points in law and in practice.

POLICY BRIEF

INTRODUCTION

For secure and democratic societies, journalists and other media actors must be able to work freely, independently, and safely. Surveillance poses a significant threat to media freedom: when journalists are targeted by surveillance, their ability to communicate securely, protect confidential sources, and pursue matters of public interest may be compromised, creating chilling effects on the exercise of freedom of expression. The growing sophistication, scale, and reach of digital surveillance technologies heighten these risks, with broader consequences for media freedom and the public's right to receive information.

In his April 2026 report to the OSCE Permanent Council, the OSCE Representative on Freedom of the Media (RFoM) warns that political pressure, technological change, economic disruption and emerging security challenges are increasingly undermining media freedom and professional journalism across the OSCE region.[1] The RFoM raises particular concerns related to mounting surveillance, including the monitoring of journalists. This phenomenon is not new and was recognized as one of the central threats to the safety of journalists already in 2018, when OSCE participating States committed themselves in Ministerial Council (MC) Decision No. 3/18 to refraining from arbitrary or unlawful interference with journalists' encryption, anonymity and communications.[2]

Rapid advances in digital surveillance are expanding the scale, sophistication and impact of surveillance against journalists and

1 *OSCE (24 April 2026) Report by the OSCE Representative on Freedom of the Media, Ambassador Jan Braathu. Available at https://rfom.osce.org/representative-freedom-media/663478 [Accessed 6 August 2026].*

2 *OSCE (2018) Ministerial Council Decision No. 3/18 on the Safety of Journalists. Vienna: OSCE.*

media workers, risking a severe chilling of independent journalism as a result. Advanced surveillance methods span communications interception, traffic and subscriber data requests, geolocation tracking and cloud-data access, including through spyware (documented in recent years against journalists in States including Italy, Spain, Armenia and Azerbaijan, among others[3]), biometric identification, artificial intelligence-assisted analytics and increasingly sophisticated capabilities for data collection, analysis and interception. This evolving landscape highlights the pressing need for full implementation of OSCE commitments on the safety of journalists, and at the same time challenges the legal, technical and institutional safeguards – where they exist – designed to protect journalists and media freedom.

International law does not prohibit surveillance outright: States may have legitimate aims in preventing and investigating serious crime and protecting national security, provided the surveillance measures are conducted on a lawful, individualized basis, are necessary and proportionate, and subject to independent oversight, they can serve that interest without violating human rights standards. Highly intrusive tools, above all spyware capable of full and covert device access, however, raise a distinct

---

3 The Citizen Lab (12 June 2025) Graphite Caught: First Forensic Confirmation of Paragon's iOS Mercenary Spyware Finds Journalists Targeted. Available at https://citizenlab.ca/research/first-forensic-confirmation-of-paragons-ios-mercenary-spyware-finds-journalists-targeted. [Accessed 1 September 2026]; The Citizen Lab (18 April 2022) CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru. Available at https://citizenlab.ca/research/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/. [Accessed 1 September 2026]; Amnesty International (25 May 2023) Armenia/Azerbaijan: Pegasus spyware targeted Armenian public figures amid conflict. Available at https://www.amnesty.org/en/latest/news/2023/05/armenia-azerbaijan-pegasus-spyware-targeted-armenian-public-figures-amid-conflict. [Accessed 1 September 2026]; The Citizen Lab (25 May 2023) Armenia-Azerbaijan Conflict Pegasus Infections – Technical Brief [1]. Available https://citizenlab.ca/research/cr1-armenia-pegasus. [Accessed 1 September 2026].

concern: their scale and covertness indicate a disproportionate interference with privacy, freedom of expression and freedom of association, particularly when deployed against journalists and their sources. This policy brief addresses undue, arbitrary or illegitimate surveillance of journalists and their sources, that affects media freedom, or that otherwise undermines the media's public interest function, in particular surveillance that lacks legal basis, individualized justification or independent oversight, or is disproportionate to its aim, including through the use of such highly intrusive tools. Throughout this brief, "arbitrary or unlawful" follows the language of Art. 17 International Covenant on Civil and Political Rights and OSCE MC Decision No. 3/18: surveillance may be arbitrary even when it is authorized by domestic law, if it is not necessary, proportionate, predictable and subject to effective oversight.

Emerging technologies have transformed surveillance from the interception of individual communications to the large-scale collection, analysis and inference of information about journalists, their sources and their professional networks. At the same time, technologies that strengthen journalists' security, including end-to-end encryption, Virtual Private Networks (VPNs) and other secure communications and security practices, have become even more important in protecting against undue surveillance and thus safeguarding media freedom, particularly when considering a substantial amount of journalistic work entails digital components, making professional practices more vulnerable. This policy brief, therefore, aims to examine whether existing legal, technical and institutional safeguards – acknowledging that such safeguards often lack proper implementation – remain fit for purpose as surveillance technologies and tactics evolve. It assesses how these technologi-

cal developments affect the implementation of exist-ing protective frameworks, including principles such as prior authorization of surveillance, oversight, redress and market controls, and identifies where additional safeguards or updated approaches may be needed.

Individual cases of surveillance should not be understood in isolation, but as manifestations of a broader surveillance ecosystem sustained by interactions between States, commercial developers, digital platforms, telecommunications providers and data intermediaries. Commercial incentives increasingly shape the collection, analysis and monetization of personal data, creating economic drivers that can reinforce surveillance infrastructures beyond traditional State actors.[4] This dynamic is not confined to States with weaker rule of law records: journalists in Belgium and Germany have demonstrated that individuals, including members of the press themselves, can be located and identified within commercially available advertising and location datasets – showing that such infrastructure exposes the media regardless of which actor exploits it.[5] Left unregulated, this ecosystem is not guaranteed to remain State-controlled: Artificial Intelligence (AI) is lowering the technical and financial barriers to developing or operating intrusive surveillance capability, raising the risk that non-State actors, including criminal networks and private actors targeting journalists directly, gain access to tools previously available only to well-resourced governments.

This ecosystem is also transnational: surveillance technology developed in one State can be exported to, and deployed by, an-

4 Shoshana Zuboff (2015) Big other: Surveillance capitalism and the prospects of an information civilization. Available at https://journals.sagepub.com/doi/10.1057/jit.2015.5 [Accessed 27 July 2026].
5 Committee to Protect Journalists (27 August 2026) How mass surveillance from online advertising puts journalists at risk. Available at https://cpj.org/special-reports/how-mass-surveillance-from-online-advertising-puts-journalists-at-risk/ [Accessed 1 September 2026].

other, including States with weak rule of law, making export controls and oversight of the commercial surveillance market as necessary as regulating States' own direct use of these tools. The highest risk of surveillance is to source confidentiality, foundational to journalism and to the public's right to receive information.[6] Governments' expanded use of surveillance and interception technologies, alongside more traditional surveillance methods such as indiscriminate metadata[7] collection, device seizures, raids and physical tailing of journalists meeting sources, puts in question the ability of journalists to protect the individuals and whistleblowers who inform their reporting. AI compounds this, accelerating the automated analysis of large volumes of information and generating inferences about behaviour, relationships and professional activities.

Digital and physical surveillance reinforce each other: intercepted communications can reveal in-person meeting points and travel patterns, so source protection cannot be addressed as a purely digital problem.[8] Surveillance creates an environment that threatens not only the confidentiality of individual communications, but also journalists' ability to investigate, protect sources, build trust and perform their democratic function.

Moreover, illegitimate surveillance rarely operates in isolation; it typically forms part of an interlocking toolkit of legal, digital, eco-

6 OSCE Representative on Freedom of the Media (2023) Communiqué No. 1/2023. Vienna: OSCE.

7 Metadata, specifically communications metadata, is information about a communication sent or received rather than its content: who communicated with whom, when and for how long, from which location, and, in the case of email, the subject line. Metadata can be particularly revealing, potentially allowing a third-party like law enforcement or another government entity to infer details about the substance of that communication even without having access to the content itself.

8 OSCE Representative on Freedom of the Media (2020) Safety of Journalists Guidebook. Available at https://rfom.osce.org/sites/default/files/f/documents/7/7/469758.pdf [Accessed 27 July 2026].

nomic and physical pressure to intimidate and silence journalists. Strategic Lawsuits Against Public Participation (SLAPPs), rising across the OSCE region, are one example of these complementary tactics, intended to intimidate, exhaust and financially burden journalists to discourage investigative reporting.[9] OSCE Ministerial Council Decision No. 3/18 calls on States to prevent defamation law from "effectively censor[ing] journalists".[10]

Technology-facilitated online violence and harassment frequently accompanies surveillance, disproportionately affecting women journalists: a 2025 survey by UN Women and the International Center for Journalists found 75 per cent of women journalists surveyed had faced online violence while working, often in co-ordinated misogynistic attacks with measurable effects on their mental health and credibility (both individually and among journalists more broadly).[11] Emerging technologies, including Generative AI, are increasingly amplifying these harms by enab-

---

9 OSCE Representative on Freedom of the Media (23 November 2021) Special Report: Legal Harassment and Abuse of the Judicial System Against the Media. Available at https://rfom.osce.org/sites/default/files/f/documents/c/f/505075_0.pdf [Accessed 27 July 2026]; OSCE Representative on Freedom of the Media (24 April 2026), Regular Report to the Permanent Council for the period from 28 November 2025 to 23 April 2026. Available at https://rfom.osce.org/sites/default/files/documents/official_documents/2026/04/fomgal0002r1%20RFoM%20Report%201561pc.pdf [Accessed 27 July 2026] ; OSCE Representative on Freedom of the Media (10 April 2025) Regular Report to the Permanent Council for the period from 6 December 2024 to 10 April 2025. Available at https://rfom.osce.org/sites/default/files/f/documents/c/5/589592.pdf [Accessed 27 July 2026]; Coalition Against SLAPPs in Europe (2025) CASE Report 2025. Available at https://www.the-case.eu/wp-content/uploads/2026/01/CASE-2025-Report-layoutted-vf.pdf [Accessed 27 July 2026].

10 OSCE (2018) Ministerial Council Decision No. 3/18 on the Safety of Journalists. Vienna: OSCE.

11 UN Women (December 2025) Tipping point: The chilling escalation of online violence against women in the public sphere. Available at https://www.unwomen.org/sites/default/files/2025-12/tipping-point-the-chilling-escalation-of-violence-against-women-in-the-public-sphere-in-the-age-of-ai-en.pdf [Accessed 27 July 2026]; United Nations Human Rights Council "Pushed into the Shadows": Evidencing Digital Surveillance Chilling Effects and the Erosion of the Rights to Freedom of Assembly and of Association. Available at https://www.ohchr.org/sites/default/files/documents/form/digital-surveillance-chilling-effects-shadows-erosion-freedom-1-en.pdf [Accessed 27 July 2026].

ling new and more invasive forms of harassment, impersonation, synthetic media and the rapid production of abusive content. Moreover, surveillance often has discriminatory and gendered effects and can reinforce inequalities and disproportionately expose women journalists to heightened scrutiny and harm. Targeted surveillance and disclosure of personal information, such as through doxing, can undermine journalists' safety, credibility, and ability to report freely.

The risks of surveillance and other complementary intimidation tactics are often magnified for journalists working in exile, who may face transnational repression across multiple jurisdictions while also encountering legal, institutional and practical barriers to accessing protection, effective remedies and accountability. It is against this cumulative picture that the adequacy of the existing protective framework and implementation must now be assessed – and strengthened.

Existing frameworks to protect journalists against undue surveillance remain conceptually valid; however, they are inconsistently implemented even for traditional forms of surveillance, and are absent altogether in some jurisdictions and contexts. Rapid advancements in surveillance technologies now require States to reassess and operationalize these frameworks in line with their underlying human rights obligations, so that they deliver the protection and accountability they were designed to guarantee amid increasingly sophisticated, including AI-enabled surveillance. It is thus essential to both assess and protect against the cumulative risks of digital surveillance, source exposure, gendered targeting, legal harassment and transnational reach, rather than evaluating each in isolation. In this context, particular attention needs to be given to the often-interconnected nature of, and emerging threats from AI-enabled

surveillance and technology-facilitated violence, specifically as they target women, marginalized and exiled journalists.

The need to update protection mechanisms (and design law enforcement capabilities on an ongoing basis in line with human rights) has also been recognized in recent international documents. The 2025 Joint Declaration on AI, Freedom of Expression and Media Freedom by the international free expression mandate holders, for example, calls on States to refrain from using digital surveillance technologies against journalists, human rights defenders and civil society as a tool of silencing, and warns more broadly that AI-driven surveillance, if deployed without adequate safeguards, can be used to target people on discriminatory grounds, a caution that traditional safeguards, designed for narrower, human-directed surveillance, were not built to anticipate.[12] The UN Special Rapporteur on counter-terrorism has similarly warned that intrusive technologies, including AI and spyware, risk normalizing exceptional surveillance powers, and called for minimum human rights standards governing their development and use.[13] Safeguards, most notably the extension of source protection beyond non-disclosure to cover inference, are particularly important where surveillance is justified by counter-terrorism or national security: powers must be necessary, proportionate and accountable, and must not erode the trust and co-operation of journalists, civil society and communities on which effective security also depends.

---

12 UN, OSCE, OAS and ACHPR (2025) Joint Declaration on AI, Freedom of Expression and Media Freedom. Available at https://www.ohchr.org/sites/default/files/documents/issues/expression/statements/2025-10-24-joint-declaration-artificial-intelligence.pdf [Accessed 27 July 2026].

13 Fionnuala Ní Aoláin (2023) Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism (A/HRC/52/39). Available at https://docs.un.org/en/A/HRC/52/39 [Accessed 27 July 2026].

In order to uphold international human rights obligations, the impact of developing technologies on these obligations need to be continuously assessed. In this context, considerations should be given to different safeguard regimes that may apply depending on the State agency deploying surveillance tools. Transparency, where feasible, can be a powerful tool to increase accountability. Particularly informative are regularly published reviews of the impact and of the crime prevention or detection value of law enforcement interventions that were enabled by surveillance technologies.

Acknowledging that surveillance can affect media freedom beyond direct interventions to uncover journalistic sources, this brief highlights the need to understand surveillance broadly – the collection or interception of data – regardless of the technologies and capabilities used. It recognizes the need to adopt higher standards when measures risk interfering with journalistic functions, exposing journalistic sources, or otherwise affecting media freedom. Additional procedural safeguards and justifications should be documented whenever surveillance measures foreseeably interfere with journalistic functions as soon as such knowledge is gained, irrespective of whether direct surveillance measures are targeting a journalist, their source, or persons close to the journalist or their reporting. For this reason, the policy brief and action points refer to surveillance affecting media freedom and not solely surveillance targeting journalists directly.

COMMITMENTS AND LEGAL BACKGROUND

Privacy is essential to freedom of expression, media freedom, and democracy; surveillance of journalists therefore engages two intersecting rights: freedom of expression – including media freedom – and the right to privacy, and, through its chilling effect, also affects the public's right to receive information. These rights are recognized and protected across binding law, political commitments and soft law.

At the international level, the International Covenant on Civil and Political Rights (ICCPR) protects freedom of expression (Art. 19) and freedom from arbitrary or unlawful interference with privacy (Art. 17). Read together and interpreted through General Comment No. 34, these provisions require States to protect journalists and safeguard source confidentiality.[14]

Under the Council of Europe's framework, Art. 8 and 10 of the European Convention on Human Rights (ECHR) provide equally binding obligations, accompanied by the jurisprudence of the European Court of Human Rights (ECtHR) developed alongside increasingly sophisticated surveillance. Goodwin v. UK (1996) and Sanoma Uitgevers v. Netherlands (2010, Grand Chamber) established that source-disclosure orders require prior review by an independent body weighing public interest against source protection. Telegraaf Media v. Netherlands (2012) extended this to covert surveillance used to unmask a source, requiring independent judicial control in a field "where abuse is potentially so easy". Big Brother Watch v. UK (2021, Grand Chamber) addressed bulk interception rather than targeted journalist surveillance, but confirmed source protection as a cornerstone of

14 UN Human Rights Committee (2011) General Comment No. 34, Article 19: Freedoms of Opinion and Expression. Geneva: OHCHR.

Art. 10 and required prior authorization wherever a “strong selector” targets a journalist, treating incidental “bycatch” more leniently, since it cannot be authorized in advance. This doctrine, developed for interception warrants and bulk-collection regimes, does not translate directly to on-device spyware, which grants real-time access to cameras, microphones, encrypted communications and location data. Although the ECtHR has yet to rule on a confirmed spyware infection of a journalist, litigation elsewhere illustrates the scale of the issue: a US federal court found NSO Group liable in December 2024 in litigation over Pegasus's use against roughly 1,400 WhatsApp users, at least 100 of whom were journalists and human rights defenders.[15]

The EU's response, through the European Media Freedom Act (EMFA), is the first binding instrument addressing surveillance and spyware against journalists, albeit a narrow one.[16] EMFA Art. 4 requires a justification test, recognizing legitimate security reasons for spyware use, subject to a higher threshold: Member States may deploy spyware to investigate offences listed in the European Arrest Warrant Framework Decision, carrying a three-year custodial threshold, or other “serious crimes” carrying a five-year threshold as defined by national law, with retrospective authorization permitted in “duly justified exceptional and urgent cases”.[17] Because the five-year threshold and its list of qualifying offences are set by each Member State's own law, the provision is exposed to significant regulatory fragmentation. The personal scope of the EMFA provision, limited to 'media service providers'

---

15 Amnesty International (7 May 2025) Global: Ruling against NSO Group in WhatsApp case a “momentous win in fight against spyware abuse”. Available at https://www.amnesty.org/en/latest/news/2025/05/ruling-against-nso-group-in-whatsapp-case-a-momentous-win/ [Accessed 27 July 2026].

16 European Union (2024) Regulation (EU) 2024/1083 (European Media Freedom Act). Official Journal of the European Union.

17 Ibid.

and connected persons, is narrower than the Council of Europe's standard (discussed below). Moreover, it leaves the outsourcing of surveillance to private contractors unaddressed, thereby creating a significant residual risk.

The Council of Europe's standard is broader in scope, albeit legally non-binding. CM/Rec(2016)4 offers comprehensive guidance across prevention, protection, prosecution and promotion, built on the positive-obligation doctrine derived from Art. 10 case law.[18] Its scope extends to "other media actors", including citizen journalists, bloggers, academics and whistleblowers, making it the more comprehensive standard even though it is limited in enforcement as a soft law instrument.

The OSCE commitment goes furthest in naming the risk. In OSCE MC Decision No. 3/18, OSCE participating States commit themselves to refrain from arbitrary or unlawful interference with journalists' encryption and anonymity and from arbitrary or unlawful surveillance.[19] RFoM Communiqué No. 1/2023 operationalizes these commitments, recognizing that some surveillance tools may be irreconcilable with media freedom altogether due to the risks and challenges brought by new technology.[20]

At the same time, some regional frameworks present challenges from a human rights perspective, including the Shanghai Cooperation Organisation (SCO), whose standards relevant to the conduct of surveillance in the context of terrorism, extremism

---

18 Council of Europe (2016) Recommendation CM/Rec(2016)4 of the Committee of Ministers to member States on the protection of journalism and safety of journalists and other media actors. Strasbourg: Council of Europe.

19 OSCE (2018) Ministerial Council Decision No. 3/18 on the Safety of Journalists. Vienna: OSCE.

20 OSCE Representative on Freedom of the Media (2023) Communiqué No. 1/2023. Vienna: OSCE.

and information security may be invoked by its Member States – including the OSCE participating States Russia, Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan and Belarus. For example, these standards include data-sharing mechanisms among intelligence services of participating States that make no reference to procedural safeguards for the handling of personal data or transparency. These standards have been criticized for not aligning with international human rights law. The Office for Democratic Institutions and Human Rights (ODIHR), for instance, expressed concerns in its 2020 note regarding the founding Shanghai Convention's definitions of "separatism" and "extremism", which are vague, overbroad and left to each State's own national definition, with no reference to human rights, due process or independent oversight.[21] When SCO Member States invoke these standards to justify surveillance activities, including of journalists, the underlying framework does not itself guarantee compliance with international human rights law and cannot, on its own, provide a legal basis for surveillance within the OSCE region. At the same time, civil society organizations have documented an intensifying pattern of digital repression against journalists and media workers across Central Asia, including in Kazakhstan and Kyrgyzstan.[22]

On the global level, the UN Plan of Action on Safety of Journalists, several UN General Assembly and UN Human Rights Council re-

21 OSCE (21 September 2020) Note on the Shanghai Convention on Combating Terrorism, Separatism and Extremism. Available at https://odihr.osce.org/odihr/467697 [Accessed 31 August 2026].

22 International Partnership for Human Rights (15 October 2025) Kyrgyzstan: UN Experts Warn of "Chilling" Impact as Assault on Media, Journalists and Activists Intensifies. Available at https://iphronline.org/articles/kyrgyzstan-un-experts-warn-of-chilling-impact-as-assault-on-media-journalists-and-activists-intensifies/ [Accessed 1 September 2026]; International Partnership for Human Rights (11 May 2026) Central Asia: Escalating Digital Repression Threatens Civic Space and Free Expression. Available at https://iphronline.org/articles/central-asia-escalating-digital-repression-threatens-civic-space-and-free-expression [Accessed 1 September 2026]

solutions and the 2024 Pact for the Future illustrate that surveillance risks are global concerns.[23] The 2023 Joint Declaration on Media Freedom and Democracy and the Office of the United Nations High Commissioner for Human Rights (OHCHR)'s 2022 spyware report call for export controls and accountability, while the Pall Mall Process represents a non-binding parallel effort to advance accountability, precision, oversight and transparency in the commercial cyber-intrusion market that supplies these tools in the first place.[24]

This regulatory and policy architecture outlines core safeguards to protect journalists from undue surveillance. These guardrails include independent ex ante authorization, transparency and accountability mechanisms. Two open questions follow: the first, addressed throughout this brief, is whether that architecture, built for traditional interception, is sufficiently calibrated to the scale, covertness and power asymmetry created by contemporary surveillance tools. The answer this brief develops section by section is that a deliberate reinterpretation of existing protection frameworks is necessary to ensure they stand the test of modern and technology-assisted surveillance and thus enforce

23 UNESCO (no date) UN Plan of Action on the Safety of Journalists and the Issue of Impunity. Available at https://www.unesco.org/en/safety-journalists/un-plan-action [Accessed 27 July 2026]; United Nations Office of the High Commissioner for Human Rights (no date) Resolutions: OHCHR and the safety of journalists. Available at https://www.ohchr.org/en/safety-of-journalists/resolutions [Accessed 27 July 2026]; United Nations (2024) Pact for the Future, Global Digital Compact and Declaration on Future Generations. Available at https://www.un.org/sites/un2.un.org/files/sotf-pact_for_the_future_adopted.pdf [Accessed 27 July 2026].

24 UN, OSCE, OAS and ACHPR (2 May 2023) Joint Declaration on Media Freedom and Democracy. Available at https://www.ohchr.org/sites/default/files/documents/issues/expression/activities/2023-JD-Media-Freedom-and-Democracy.pdf [Accessed 27 July 2026] ; United Nations Human Rights Council (4 August 2022) The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights. Available at https://docs.un.org/en/A/HRC/51/17 [Accessed 27 July 2026]; France and United Kingdom (February 2024) Pall Mall Process Declaration. Available at https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities [Accessed 28 July 2026].

the commitments to safety of journalists and media freedom.

The second question is institutional rather than technological: these safeguards presuppose institutional conditions (rule of law, judicial independence, separation of powers) that are under strain across the OSCE region.[25] Where they do not hold, a legal test that reads identically on paper cannot be assumed to deliver the same protection in practice: a formally correct authorization procedure offers little safeguard if the body applying it is not genuinely independent of the executive seeking to surveil. Surveillance activity itself, not only the safeguards meant to constrain it, may consequently differ according to the degree of rule of law and separation of powers in the surveilling State. Where rule of law constraints are strained but still functional, surveillance may proceed nominally through a legal architecture that is too permissive, under-resourced, or deliberately hollowed out; where separation of powers has broken down more fundamentally, surveillance need not engage that architecture at all, because the institutions meant to authorize, oversee, or remedy it are themselves captured or non-independent. The same threshold, authorization and oversight standards therefore apply throughout this brief regardless of institutional context, but their capacity to actually constrain State conduct does not.

Under the functional concept, legal safeguards extend to all persons performing a journalistic function (freelancers, bloggers, citizen journalists, editorial and technical staff) as well as their sources, consistently with the functional conception of journalism in Human Rights Committee General Comment No. 34. As emphasized in the introduction, surveillance measures can

---

25 OSCE Office for Democratic Institutions and Human Rights (no date) PART 1 - Creating strong democratic institutions based on rule of law to increase public trust. Available at https://odihr.osce.org/odihr/attachment/662770 [Accessed 27 July 2026].

negatively affect media freedom even when measures do not directly target an individual journalist. A robust legal framework with procedural safeguards is needed when surveillance measures knowingly or predictably risk intercepting journalistic sources or the subject matter of journalistic work. More broadly, it is essential that States recognize privacy as essential to freedom of expression, media freedom, and democracy.

SURVEILLANCE THRESHOLD

For the purpose of this brief, State surveillance encompasses surveillance undertaken by law enforcement authorities for criminal investigative purposes as well as by intelligence, security and other public authorities for national security or intelligence purposes. The legal threshold preventing surveillance against journalists and the corresponding safeguards should attach to the nature and impact of the interference, rather than to the institutional classification of the authority conducting it.

International human rights law permits surveillance only exceptionally, in view of the higher human rights risk of surveillance against journalists, given the direct interference with expression and source confidentiality. Interference must satisfy legality, legitimate aim, necessity and proportionality, as well as non-discrimination. It further requires procedural safeguards including prior judicial authorization by a court or other independent authority, narrow targeting, time and scope limits, notification, oversight and remedies. These conditions are rarely met and, for some tools, arguably cannot be: the RFoM has noted in Communiqué No. 1/2023 that it seems “very hard to imagine that the use of extremely pervasive and intrusive spyware on journalists and other media actors can ever be considered compatible with the principles agreed upon in the OSCE”. Equally,

the European Data Protection Supervisor has stated that full-device-access spyware like Pegasus is “highly unlikely” ever to satisfy proportionality, since the interference affects the essence of the right to privacy.[26]

Surveillance methods span a spectrum of intrusiveness. Interception, subscriber/traffic data requests, geolocation records and cloud access can expose confidential networks without ever touching content. Far more intrusive are commercial spyware tools (Pegasus, Predator, Graphite), which exploit vulnerabilities, often via zero-click attacks, for covert, continuous device access.[27] Comparably invasive access can also be achieved through physical rather than remote means: in Serbia, for example, forensic-extraction tools were used to exploit device vulnerabilities and unlock a journalist's phone during police detention, enabling covert spyware installation.[28] In Belarus, as another example, the state security service similarly used physical device access during interrogation to implant spyware capable of live microphone recording, screen capture and exfiltration of encrypted messaging data.[29] Journalists elsewhere also face AI-sharpened phishing, social engineering, insider abuse and stalkerware, with authorities increasingly combining data sources with AI-assisted analytics to reconstruct

---

26 European Data Protection Supervisor (15 February 2022) Preliminary Remarks on Modern Spyware. Available at https://www.edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf [Accessed 27 July 2026].

27 Samar Al Halal (March 2026) Global Surveillance of Journalists: A Technical Mapping of Tools, Tactics, and Threats. Available at https://www.ifj.org/fileadmin/Global_Surveillance_of_Journalists_-__A_Technical_Mapping_of_Tools__Tactics__and_Threats_JD_210426.docx.pdf [Accessed 27 July 2026].

28 Amnesty International (16 December 2024) Serbia: 'A Digital Prison' - Authorities using spyware to unlawfully hack journalists and activists. Available at https://www.amnesty.org.uk/latest/serbia-digital-prison-authorities-using-spyware-unlawfully-hack-journalists-and/ [Accessed 1 September 2026].

29 Reporters Without Borders (17 December 2025) Exclusive: RSF uncovers new spyware from Belarus. Available at https://rsf.org/en/exclusive-rsf-uncovers-new-spyware-belarus [Accessed 1 September 2026].

journalistic activity from metadata alone.[30] The legal assessment of surveillance should therefore focus on the degree of intrusion, the specificity of targeting, and likely impact, not on the technology alone. Applied to the most intrusive end of that spectrum, this yields a clear conclusion: covert surveillance of journalists, above all highly intrusive spyware, should be understood as not being in line with international human rights standards and OSCE commitments and thus presumptively prohibited. If technologies or tools are disproportionate by design, they should per se not be developed, produced, sold, imported, exported, or used, whether developed in-house, by contractors, or acquired commercially. If not a priori disproportionate, States should still ensure that journalists are not targeted with surveillance solely for their journalistic work or to identify journalistic sources. Special safeguards are also needed to ensure that any captured data capable of identifying sources is properly identified, isolated, and destroyed.

Access to stored communications, metadata, contacts, browsing and location history, and particularly invasive tools like spyware that gives near-total device access, now let authorities reconstruct networks and identify sources without ever compelling direct disclosure. Biometric identification compounds this, through techniques such as facial recognition against a reference database, gait analysis from a person's distinctive walk and voice-print matching from acoustic characteristics. None requires real-time interception; they can run against footage or audio already in storage, with no discrete collection event for an interception-based authorization framework to attach to. Source protection must therefore extend beyond preventing compelling

30 *See footnote 27.*

testimony to safeguarding information revealed indirectly through surveillance. This should include both systems that are purpose-built for surveillance and those repurposed from a commercial product.

Already in 2021, UN Special Rapporteurs called for a global moratorium on the sale and transfer of surveillance technology pending robust human rights safeguards.[31] The RFoM Communiqué in 2023 clearly concludes that the most invasive spyware tools are so pervasive that their use against journalists is hard to reconcile with OSCE commitments in any circumstance, and urges participating States to refrain from such use altogether rather than treating it as subject to the threat-based exception that applies to surveillance technology generally.[32] While international law does not yet impose an explicit categorical ban, the cumulative burden of necessity, proportionality and source protection is so difficult for intrusive commercial spyware to satisfy that its use against journalists should be treated as incompatible with States' human rights obligations.

Building on the gaps identified, this brief highlights the need for robust legal frameworks for agencies performing surveillance, be it law enforcement, intelligence or otherwise. Any surveillance measure requires a legal basis, whatever the technology, covering indirect surveillance (metadata, aggregation, AI-assisted inference), non-digital methods (compelled passcode or biometric unlocking, device search and seizure) and commercial cyber-intrusion capabilities. The legal framework should also ensure that buying commercially available datasets on

---

31 United Nations Human Rights Office of the High Commissioner (12 August 2021) Spyware scandal: UN experts call for moratorium on sale of "life threatening" surveillance tech. Available at https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening [Accessed 27 July 2026].

32 OSCE Representative on Freedom of the Media (2023) Communiqué No. 1/2023. Vienna: OSCE.

outsourcing surveillance cannot circumvent these safeguards. Any surveillance needs to be permitted only where prescribed by law, demonstrably and exclusively justified by a legitimate aim, and necessary and proportionate, including during emergencies and derogations. Technical capability or convenience is not a legitimate aim, and blanket "national security" or "public order" exceptions must not be adopted. Surveillance must be a last resort once other investigative means are exhausted, supported by a documented human rights impact assessment, with additional justification and mandatory consideration of media freedom, not only privacy, where journalistic functions or sources may be affected. Moreover, surveillance powers must never be used to manipulate, plant or delete data on a target device, or to fabricate or alter AI-assisted inferences used against a journalist.

AUTHORIZATION

Lawful surveillance requires detailed, specific, substantive prior independent authorization, by a judicial or other independent authority. This requirement should apply irrespective of whether surveillance is sought by a law enforcement authority in the context of a criminal investigation or by an intelligence or security service for national-security purposes. Generic, blanket, or solely internal authorizations are insufficient as they risk overbroad or indiscriminate surveillance. Authorization must be independent and free from political or administrative influence. It must also clearly define the scope and objectives of surveillance, including its targets, the data collected and its duration, and must assess necessity and proportionality against the legitimate aim pursued. The authorizing body should receive enough technical information about the tool and its specifications, to as-

sess for itself whether it is the least invasive means available, and it should apply the threshold to combinations of data sources analyzed together, not only to individual surveillance tools in isolation. Authorizing bodies require sufficient technical expertise (internally or through appropriate advice), and they must require a human decision-maker to be able to articulate the basis for an AI tool's output at the point of authorization; an authorization that cannot be meaningfully explained fails a "specific, substantive" test by definition.

The authorization needs to be given prior to the surveillance measure, be individualized, tied to a specific purpose, be time-bound and limited by data minimization, retention limits and mandatory deletion. Analytical methods require their own necessity and proportionality demonstration, distinct from the authorization for the underlying collection (separate for each stage). Authorizing interception of a journalist's communications does not thereby authorize an algorithm to infer their source network from the resulting metadata. Source protection should extend beyond non-disclosure to cover inference so that surveillance-derived information is not used to identify, investigate or prosecute a source even if the underlying surveillance was itself lawful.

Where a person performing a journalistic function is targeted, or where a surveillance measure is likely to reveal confidential journalistic material or identify the source, the requesting body or agency performing the surveillance must demonstrate the necessity and proportionality of the measure before an independent judicial authority. Executive, ministerial or internal agency approval alone should not satisfy this standard. Where the agency performing the surveillance or the requesting body maintains that surveillance of a journalist relates to matters un-

related to their journalistic activity, that distinction must itself be demonstrated as part of the authorization process. It should not be for the requesting law enforcement or intelligence agency alone to determine that the activity is separate from the person's journalistic function.

So far, designing authorization for the AI era remains open and largely unaddressed: AI-enabled tools blur "targeted" versus "systemic" surveillance and can defeat case-by-case judicial review unless authorization is redesigned around actual technical capability rather than formal legal label. No court or standard-setter has yet articulated what "specific, substantive" authorization means where the targeting decision is itself machine-assisted, a challenge compounded when AI-assisted decision-making comes into play. The potential of an increasing use of AI in judicial decision-making raises serious concerns regarding impartiality as the complexity and the continuous, rapid development of surveillance systems may prompt judges and other parties to use AI tools to help assess whether to authorize specific surveillance measures.

Existing protections do not yet cover all commercial cyber-intrusion capabilities (CCICs) as defined by the Pall Mall Process, including AI-enhanced variants and future technologies not yet in existence. Any new protection framework must be designed to address the expanding technological capabilities that are paired with decreasing detectability, given AI's expansion of autonomous vulnerability-discovery and exploit-operationalization capabilities.

OVERSIGHT

Oversight must be continuous, independent, empowered to act on its own initiative, with the legal instruments necessary to detect and combat abuse.[33] It must include strict controls on the authorization, execution and review of surveillance measures and keep pace with the tool itself: technical audits require dedicated technical capacity, not merely legal review of authorizing paperwork. That capacity must extend to how surveillance data is analyzed after collection: where AI systems aggregate, cross-reference, or infer from previously collected data, whether to identify a source, reconstruct a network, or select a future target, oversight must reach that analytical stage directly, not only the initial authorized collection.

Greece's Predatorgate scandal demonstrates how oversight can be compromised at its most basic level. In March 2021, before the scandal broke, Greece's parliament passed a retroactive amendment stripping the Hellenic Authority for Communication Security and Privacy (ADAE), the body overseeing surveillance, of its power to ever notify a person placed under national-security surveillance, even after that surveillance ended.[34] When it emerged that journalist Thanasis Koukakis had been surveilled with Predator spyware, and that freelance journalist Stavros Malichoudis had been wiretapped by Greece's intelligence service, that amendment left victims no legal path to learn what

33 Amnesty International (26 February 2025) Poland: Written submissions filed to the European Court of Human Rights in the case of Krzysztof Brejza v. Poland and 8 Other Applications. Available at https://www.amnesty.org/zh-hans/documents/eur37/9082/2025/en/ [Accessed 27 July 2026].

34 Reporters Without Borders (12 October 2022) Greece: At a meeting with RSF, the government commits to ban the use of spyware. Available at https://rsf.org/en/greece-meeting-rsf-government-commits-ban-use-spyware [Accessed 27 July 2026].

happened. Greece's Council of State ruled the amendment unconstitutional in April 2024.[35]

For oversight bodies to fulfil their independent role, they must maintain dedicated technical capacity sufficient to assess spyware's technical characteristics and intrusion capabilities as well as to audit the training data, decision logic and error rates of any AI-assisted analytical tool used in an operation, in addition to the spyware or surveillance tool. Oversight bodies should have access to persistent, tamper-evident audit logs of every query and inference made based on authorized surveillance measures. Moreover, disaggregated annual public reporting should be provided to separate journalist-specific surveillance from general oversight statistics and to report AI-assisted analytics as a category distinct from device-level collection.

Oversight bodies can themselves become surveillance targets or be captured in certain contexts. A striking example is Citizen Lab's 2026 confirmation that Stelios Kouloglou, then a substitute member of the European Parliament's PEGA Committee of Inquiry, had been infected with Pegasus twice during the committee's active inquiry.[36] Moreover, in the absence of any bin-

35 Safety of Journalists Platform (19 April 2022) Journalist Thanasis Koukakis Targeted With Spyware Predator. Available at https://fom.coe.int/en/alerte/detail/107637431 [Accessed 27 July 2026]; Media Freedom Rapid Response (19 September 2023) Greece: Refugee reporting in times of surveillance. Available at https://www.mfrr.eu/greece-refugee-reporting-in-times-of-surveillance/ [Accessed 27 July 2026] ; Human Rights Watch (10 April 2024) Greek Court Deems Surveillance Powers Unconstitutional Court Demands Stricter Safeguards on State Monitoring. Available at https://www.hrw.org/news/2024/04/10/greek-court-deems-surveillance-powers-unconstitutional [Accessed 27 July 2026].

36 The Citizen Lab (3 July 2026) Espionage Against the European Parliament: Member of Committee Investigating Spyware Hacked with Pegasus. Available at https://citizenlab.ca/research/member-of-committee-investigating-spyware-hacked-with-pegasus/ [Accessed 27 July 2026] ; European Parliament (no date) Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA) – Members. Available at https://www.europarl.europa.eu/committees/en/archives/9/pega/members [Accessed 27 July 2026].

ding, cross-border mechanism for investigating and sanctioning abuse after the fact, oversight bodies' decisions can only have limited impact. A further challenge is brought by AI-assisted analysis: where AI tools are used to aggregate data, cross-reference sources, or flag targets for further collection, that analytical layer typically sits outside any existing oversight mandate, which reviews the authorization and execution of collection, not what is done with the data afterward. As a result, an oversight body can audit a spyware warrant in full and still have no visibility into the algorithm that used the resulting data to identify a source.

REDRESS: NOTIFICATION, SUPPORT, EFFECTIVE REMEDIES

Accountability for arbitrary or unlawful surveillance of journalists remains the exception rather than the rule: the secrecy inherent to surveillance, combined with the barriers to standing, evidence and remedy documented throughout this brief, as well as interlinkages with political power, has produced a climate of near-impunity in which victims rarely obtain redress and perpetrators are rarely held to account.

Effective redress requires an accessible forum and a meaningful supply of remedies, embedded in a rule of law system. Notification is both a State obligation and the most direct route to challenging arbitrary or unlawful surveillance, which, given its secret nature, is very difficult to detect and challenge without it. Notification and access to effective remedy must not depend on whether surveillance was conducted pursuant to criminal-procedure, intelligence or national-security functions. However, remedies cannot depend on notification being given, as in prac-

tice it may be delayed, withheld or never provided. The European Parliament's PEGA recommendations call for mandatory notification for both targeted individuals and incidentally affected third parties, paired with independent post-hoc oversight and access to legal redress.[37]

Notification delay should be permissible only where a judicial or other independent authority finds that immediate notification would seriously jeopardize the legitimate aim of the measure.[38] Any delay should also be capped by fixed time limits, with any extension requiring further judicial authorization. Notification must include sufficiently detailed information: at minimum, the fact, date of authorization, duration of surveillance, the warrant authorizing it, the data obtained and how it was used, the date of its deletion and the available avenues for redress. In practice, formal State notification is often missing entirely, or is preceded or supplemented by private-sector actors: Apple's threat notifications are routinely channelled to Access Now's Digital Security Helpline and Citizen Lab, which provide forensic verification, device triage and support.[39] While this fills an important practical gap, it cannot substitute for States' legal notification obligations.

---

37 European Parliament (15 June 2023) Recommendation to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2023/2500(RSP)). Available at https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.html [Accessed 27 July 2026].

38 Ibid.

39 Access Now (no date) Access Now's Digital Security Helpline and Apple threat notifications. Available at https://www.accessnow.org/help/access-nows-digital-security-helpline-and-apple-threat-notifications/ [Accessed 27 July 2026]; The Citizen Lab (12 June 2025) Graphite Caught: First Forensic Confirmation of Paragon's iOS Mercenary Spyware Finds Journalists Targeted. Available at https://citizenlab.ca/research/first-forensic-confirmation-of-paragons-ios-mercenary-spyware-finds-journalists-targeted/ [Accessed 27 July 2026].

Victims should have access to the collected material to understand the scope of the interference and effectively seek relief: cessation of arbitrary or unlawful surveillance, deletion of arbitrarily or unlawfully obtained data, compensation and accountability for those responsible. That responsibility rests first with the State, not the vendor: it is the State that authorizes, deploys and benefits from surveillance, and it is its legal system that determines whether a remedy exists at all. It is thus essential to have annual transparency reports on the number and scope of surveillance authorizations, and to ensure that victims, including journalists, can obtain legal remedy and compensation directly from the State, not only through litigation against vendors. The most consequential litigation so far has targeted vendors rather than the authorizing States, not because vendors bear greater responsibility, but because secrecy around authorization may make the State itself an unreachable defendant.[40] Victims can identify the spyware that infected their device, but rarely the official who approved its use, on what legal basis or with what oversight: vendor litigation is a symptom of State opacity, not a substitute for State accountability.

Effective remedies should be a joint obligation of the State and any vendor involved in the surveillance, so that a journalist harmed by arbitrary or unlawful surveillance can obtain meaningful relief regardless of whether the responsible conduct originated with the authorizing State, a contractor, or the tool's developer.

---

40 Amnesty International (7 May 2025) Global: Ruling against NSO Group in WhatsApp case a "momentous win in fight against spyware abuse". Available at https://www.amnesty.org/en/latest/news/2025/05/ruling-against-nso-group-in-whatsapp-case-a-momentous-win/ [Accessed 27 July 2026] ; International Consortium of Investigative Journalists (26 February 2026) Greek court convicts Intellexa founder Tal Dilian, three others in wiretapping scandal. Available at https://www.icij.org/investigations/cyprus-confidential/greek-court-convicts-intellexa-founder-tal-dilian-three-others-in-wiretapping-scandal/ [Accessed 27 July 2026].

In order to enable redress, prompt notification of any surveillance measure – including AI-assisted inference of source identity or journalistic network, not only upon device infection or direct interception – to individuals targeted by arbitrary, unlawful or no-longer-necessary surveillance is crucial. Identifying a source through cross-dataset analysis of data that the State already holds, without any new collection directed at the journalist, is still surveillance in every sense that matters to source protection, and the notification and remedy architecture must account for that. Delay is justified only when (1) notification would seriously jeopardize the purpose for which the surveillance is authorized, or there is an imminent risk of danger to human life; and (2) the authorization to delay notification is granted by a competent independent authority within fixed time limits and with additional justification where national security is invoked; and (3) the person(s) affected are notified as soon as the risk is lifted as determined by a competent judicial authority. The obligation to notify rests with the State; however, independent threat-notification services must be supported and safeguarded.

Following notifications, to enable redress, it is essential that States provide access to swift, impartial and effective judicial remedies for journalists subjected to arbitrary or unlawful surveillance, including AI-assisted surveillance, covering compensation, deletion of arbitrarily or unlawfully collected or inferred data, correction of resulting inferences, restitution, rehabilitation, satisfaction and guarantees of non-repetition. To support these processes, it is particularly useful if States provide legal aid, psychosocial support and rapid-response assistance, where possible, including dedicated support for exiled journalists. Any person with reasonable grounds to suspect they have been subjected to surveillance, including inference-based

surveillance, must be able to bring a complaint to an independent body with the powers and access to information needed to investigate it, determine whether surveillance occurred and whether it was arbitrary or unlawful, and order appropriate remedies where a violation is found, irrespective of notification. Overall, transparency should be treated as a security guarantee in its own right, not a concession to it. It is thus important that States publish annual reports on the number, scope and legal basis of surveillance authorizations.

THIRD-PARTY AND TRANSNATIONAL SURVEILLANCE

In addition to the requirement placed on States by international human rights law, complemented by OSCE commitments, to establish a legal and institutional framework protecting journalists against arbitrary or unlawful surveillance by public authorities, States also bear a positive obligation to protect journalists against arbitrary or unlawful surveillance carried out by foreign States or private actors. This operates on two fronts. Externally, through export controls on commercial cyber-surveillance technology – for EU Member States, under Art. 5 of the EU Dual-Use Regulation (2021/821) – paralleled by non-EU multilateral efforts, including the US-led 2023 Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware and the Pall Mall Code of Practice, a voluntary, non-binding commitment led by France and the UK and currently endorsed by 27 States – 23 of which are also OSCE participating States (complemented by Ghana, Japan, Kosovo and the Republic

of Korea).[41] To ensure protection across borders, it is essential that States, internally, prevent, investigate and remedy arbitrary or unlawful surveillance within their jurisdiction carried out by foreign services or private entities.

This obligation is most acute for exiled journalists, who remain within reach of their State of origin's surveillance despite residing outside its territory. Effective protection of exiled journalists and other media actors depends on the host State's willingness to regard surveillance on its own soil, even by a foreign State against a foreign national or by other foreign actors, as falling within its jurisdiction in terms of prevention, investigation, and remedy, and to facilitate access to redress regardless of the victim's nationality or immigration status. To enable protection, exiled journalists and other media actors require access to effective protection and remedy against surveillance by their State of origin or other foreign actors on host-State territory, through host-State investigation, mutual legal assistance and co-operation with regional and international mechanisms. Psychosocial support can be equally relevant in such contexts as legal support, considering that continuous threats of surveillance and its potential impact – the shadow of surveillance – can be as powerful in restricting journalistic activity.

---

41 European Union (2021) Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast). Official Journal of the European Union; U.S. Department of State (22 September 2024) Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware. Available at https://2021-2025.state.gov/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/ [Accessed 27 July 2026] ; France and United Kingdom (April 2025) The Pall Mall Process: Code of Practice for States. Available at https://assets.publishing.service.gov.uk/media/68f902996a52e8a2726dc2f6/The-Pall-Mall-Process-Code-of-Practice-for-States-October-update.pdf [Accessed 28 July 2026].

PROCUREMENT, EXPORT, AND INVESTMENT

The Pall Mall Code of Practice frames the commercial cyber-intrusion capabilities (CCICs) market as an ecosystem of vulnerability researchers, exploit developers, brokers, vendors, investors and end users, rather than a single-vendor problem.[42] It commits governments to conducting due diligence across the entire supply chain.[43] However, the Pall Mall Code does not extend to cyber-intrusion capabilities developed and used in-house by governments, leaving State development largely unaddressed.[44] This gap must not be interpreted as a reason to legitimize State-run development without the same prohibitions and safeguards to it, and ensuring transparency around the tools available.

Procurement, export controls, and investment represent distinct regulatory points within the surveillance ecosystem, yet existing frameworks address them unevenly and suffer from significant implementation gaps. On procurement, the Pall Mall Code of Practice commits States to defining which entities under their jurisdiction may import, purchase, hold or use commercial CCICs, to excluding vendors that fail to meet standards of legality and human rights due diligence from government procurement, and to adopting know-your-vendor and know-your-customer practices.[45] These commitments remain voluntary. Moreover, they neither prohibit procurement of high-risk spyware nor re-

42 France and United Kingdom (April 2025) The Pall Mall Process: Code of Practice for States. Available at https://assets.publishing.service.gov.uk/media/68f902996a52e8a2726dc2f6/The-Pall-Mall-Process-Code-of-Practice-for-States-October-update.pdf [Accessed 28 July 2026].

43 Ibid.

44 Ibid.

45 Ibid.

quire notification when purchasing zero-day vulnerabilities. US Executive Order 14093 offers a binding, if narrower, example. Federal agencies may not make operational use of commercial spyware, or request or directly enable a third party to do so, where they determine, on credible information, that it poses significant counterintelligence or security risks or significant risks of improper use by a foreign government or foreign person.[46] Relevant risk factors include control of the vendor by a foreign government or person engaged in intelligence activities against the United States, and past use of its spyware by a foreign government or person against journalists, activists and dissidents.[47] The Order nonetheless governs only the US Government's own use, does not appear to reach government-built tools, allows waivers of up to one year and gives affected persons no enforceable rights.[48] Comparable controls should extend to development, export and use of all spyware by all State actors, including intelligence, law enforcement and military agencies, and their contractors, whether the tool is commercial or government-built.

CCIC vendors should be assessed against human rights and rule of law standards in procurement, excluding any vendor implicated in unlawful surveillance or lacking the transparency, oversight and remedy mechanisms required for accountability, and engaging only vendors that adhere to the UN Guiding Principles on Business and Human Rights. The same standard

---

46 The White House (27 March 2023) "Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security". Available at https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/ [Accessed 5 August 2026].

47 Ibid.

48 Ibid.

must extend to any AI-analytics vendor supplying a separate inference or target-selection layer.

On export control, the Wassenaar Arrangement, a voluntary 42-member regime whose participants include 34 OSCE participating States, has added intrusion software to its dual-use control list, but the Arrangement remains a non-binding commitment, its implementation left entirely to individual States.[49] Moreover, key countries exporting technologies used for surveillance, such as Israel, are not members of Wassenaar, aligning only through unverified self-assessment; particularly on intrusion software, Israel has adopted controls that are less stringent than those agreed in Wassenaar, allowing vendors to escape stricter licensing by relocating.[50]

Export control regimes must extend to spyware, cyber-surveillance technology and AI-enabled surveillance technology alike, including target-selection, pattern-of-life profiling and inference tools procured or licensed separately from the underlying collection tool, so a capability cannot escape control merely because it is not bundled with the spyware or interception hardware it enhances.

Where a surveillance tool has built-in AI-powered analytic capability, export licensing and procurement due diligence must treat this as triggering an additional layer of review, assessing the compounded human rights impact of the AI-enabled capability

---

49 The Wassenaar Arrangement (no date) List of Dual-Use Goods and Technologies and Munitions List. Available at https://www.wassenaar.org/control-lists/ [Accessed 28 July 2026].

50 Reuters (22 August 2019) Israel eases rules on cyber weapons exports despite criticism. Available at https://www.reuters.com/article/world/israel-eases-rules-on-cyber-weapons-exports-despite-criticism-idUSKCN1VC0XB/ [Accessed 27 July 2026]; LawFare (10 December 2025) Regulating Commercial Spyware Through Export Controls. Available at https://www.lawfaremedia.org/article/regulating-commercial-spyware-through-export-controls [Accessed 27 July 2026].

together with the underlying tool, rather than evaluating the base tool and its AI features as if they carried separate, additive risk.

At the EU level, Art. 5 of the EU Dual-Use Regulation introduced a human rights-based "catch-all" control requiring authorization for cyber-surveillance items not listed on the EU control list (Annex I) where such exports could facilitate internal repression or serious human rights violations.[51] The Regulation also requires exporters using global export authorizations to implement Internal Compliance Programmes incorporating human rights due diligence. In practice, however, enforcement falls well short.[52] The Center for Democracy & Technology Europe found inconsistent licensing standards across EU Member States, opaque decision-making, little monitoring of end use after export, and regulatory divergence enabling vendors to forum-shop for the most permissive authority.[53] Human Rights Watch likewise reported in May 2026 that the European Commission had yet to conduct its mandatory review, while national authorities routinely failed to act on known human rights risks.[54]

Investment in technologies that can be used to illegitimately surveil journalists remains even less regulated: in 2025 it emerged that the European Investment Fund had indirectly fi-

---

51 European Union (2021) Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast). Official Journal of the European Union.

52 Centre for Democracy & Technology Europe (4 December 2025) From Export Control to Unknown Exports: How the EU's Dual-Use regime falls short on tackling spyware. Available at https://cdt.org/wp-content/uploads/2025/12/CDT-Europe-Report-on-the-Dual-Use-Regulation.pdf [Accessed 27 July 2026].

53 Ibid.

54 Human Rights Watch (12 May 2026) Looking the Other Way: EU Failure to Prevent Surveillance Exports to Rights Violators. Available at https://www.hrw.org/report/2026/05/12/looking-the-other-way/eu-failure-to-prevent-surveillance-exports-to-rights [Accessed 27 July 2026].

nanced Paragon Solutions through a venture capital intermediary. Paragon's Graphite spyware was later confirmed to have been used against journalists, humanitarian workers and activists in Italy.[55] At present, no framework effectively bars grants, investment, or procurement from reaching spyware companies through subsidiaries or shell structures, requires disclosure of investors and end-user agreements, or makes human rights due diligence binding for publicly funded research. Building on the gaps identified above, this brief highlights the need for States to ensure export controls incorporate human rights due diligence and end-user verification and must close the loophole currently letting functionally equivalent AI-assisted forensic-extraction tools escape catch-all controls applied to purpose-built spyware.

Principles discussed in this section around prohibitions, authorizations, oversight, vulnerability-disclosure and export-control requirements need to be equally applied to capabilities developed by State agencies themselves. In-house or "sovereign" origin is neither an exemption nor a presumption of lawfulness.

At the same time, human rights-based regulation of private-sector surveillance is needed, including of data brokers, ad-tech location data and consumer devices such as smart home devices, drones, geotags and smart glasses. To limit chilling effects, such regulation needs to cover both purpose-built and functionally equivalent extraction tools, and be enforced, including by uphol-

55 *EUobserver (16 October 2025) European Investment Fund financed Israeli spyware company Paragon. Available at https://euobserver.com/23212/european-investment-fund-financed-israeli-spyware-company-paragon/ [Accessed 27 July 2026] ; The Citizen Lab (12 June 2025) Graphite Caught: First Forensic Confirmation of Paragon's iOS Mercenary Spyware Finds Journalists Targeted. Available at https://citizenlab.ca/research/first-forensic-confirmation-of-paragons-ios-mercenary-spyware-finds-journalists-targeted/ [Accessed 27 July 2026].*

ding companies' responsibilities under the UN Guiding Principles on Business and Human Rights.

TECHNOLOGICAL SAFEGUARDS

Safeguards must extend beyond regulating the deployment of spyware to the technical and design decisions that enable (the extent of) surveillance in the first place. When governments discover software vulnerabilities, they face a choice between disclosure and retention for offensive use – the same choice underlying "government trojan" and lawful-hacking proposals debated in several States, where authorities seek access to encrypted communications by exploiting undisclosed vulnerabilities rather than compelling decryption. Retained vulnerabilities remain exploitable by other actors, creating cybersecurity risks that extend well beyond the intended target. The Pall Mall Code of Practice refers to co-ordinated vulnerability disclosure only in the context of legitimate cybersecurity activities, and although it recommends that States establish an evaluation process for discovered vulnerabilities, it neither prescribes how decisions should be made nor creates a presumption favouring disclosure of vulnerabilities retained or acquired for CCIC purposes.[56] It would be useful to establish a binding disclosure mechanism requiring such vulnerabilities used or acquired for CCIC purposes to be disclosed unless temporary retention is independently authorized as strictly necessary and proportionate, subject to periodic review.

Safety design can and should complement legal safeguards:

---

56 France and United Kingdom (April 2025) The Pall Mall Process: Code of Practice for States. Available at https://assets.publishing.service.gov.uk/media/68f902996a52e8a2726dc2f6/The-Pall-Mall-Process-Code-of-Practice-for-States-October-update.pdf [Accessed 28 July 2026].

Apple's Lockdown Mode and Google's Android Intrusion Logging (developed with Amnesty International and Reporters Without Borders) reduce a device's attack surface and, in Google's case, preserve encrypted forensic logs even where spyware erases its traces.[57] Amnesty International's open-source Mobile Verification Toolkit (MVT) lets forensic experts examine a device after the fact of surveillance for indicators of spyware compromise.[58] All three measures remain voluntary or opt-in, however, and must be a complement – not a substitute for – binding obligations.

A commitment to safeguarding the right to privacy requires States to protect the lawful development, distribution and use of encryption and anonymity technologies, including VPNs, Tor, Signal and similar tools, as essential safeguards for secure communications. Likewise, the development, distribution or use of such technologies should neither be unduly prohibited nor restricted, nor should their use be treated as sole evidence of criminality or grounds for heightened suspicion. Moreover, protection can only be ensured if States do not mandate backdoors or knowingly maintain backdoors in encryption or other deliberate cybersecurity vulnerabilities.

Weak rule of law and separation of powers not only affect the institutions meant to oversee surveillance, but also the tools used to resist it: the encryption and anonymity technologies, including VPNs, on which journalists' security and source protection depend. In some contexts, their use has been treated

---

57 Apple (6 July 2022) Apple expands industry-leading commitment to protect users from highly targeted mercenary spyware. Available at https://www.apple.com/newsroom/2022/07/apple-expands-commitment-to-protect-users-from-mercenary-spyware/ [Accessed 27 July 2026] ; Google (12 May 2026) What's New in Android Security and Privacy in 2026. Available at https://blog.google/security/whats-new-in-android-security-privacy-2026/ [Accessed 27 July 2026].

58 Mobile Verification Toolkit (no date) Mobile Verification Toolkit. Available at https://docs.mvt.re/en/latest/ [Accessed 27 July 2026].

as evidence of criminal intent, or is even criminalized entirely, hindering journalists from using such tools for digital security and source protection. Where rule of law constraints remain respected, States may fall back on restricting or stigmatizing encryption and anonymity technologies rather than compromising them directly. In some contexts, prosecutors have treated the use of such protective measures as evidence of "clandestine" behaviour in terrorism cases, turning them into grounds for suspicion.[59] Where legal safeguards do not hold, restrictions may become unnecessary: a State can control or compromise the relevant infrastructure directly, offering or banning certain VPNs, messaging apps, or "secure" services that are State-run or State-compromised in substance while indistinguishable from a genuine safeguard in form. This logic reaches its endpoint when a State owns the infrastructure outright rather than merely accessing it.

Russia's MAX "super-app", preinstalled on every new smartphone sold in Russia since September 2025, was rolled out as authorities simultaneously degraded WhatsApp and Telegram.[60] It builds covert call recording, VPN detection and silent remote message deletion directly into consumer infrastructure, requiring no device infection and replacing secure alternatives with surveillance by design. Exiled journalists' families now fear contacting them, and Ukrainian journalists are cut off from sour-

59 For example, La Quadrature du Net (5 June 2023) Criminalization of Encryption: the 8 December Case. Available at https://www.laquadrature.net/en/2023/06/05/criminalization-of-encryption-the-8-december-case/ [Accessed 27 July 2026].

60 Digital Forensic Research Lab (21 May 2026) The domestic Russian "super-app" that could create cross-border security risks. Available at https://dfrlab.org/2026/05/21/the-domestic-russian-super-app-that-could-create-cross-border-security-risks/ [Accessed 27 July 2026].

ces in occupied territory.[61] The same pattern extends wherever the tools journalists rely on, such as a VPN, a messaging app, or a certificate authority, are supplied or controlled by an actor with an interest in defeating them: users cannot distinguish a safeguard from its opposite, and adopting protective measures becomes a vector for surveillance rather than a defence against it.

Legal and technical safeguards are therefore only meaningful where governments do not undermine them, including on national security grounds, either by restricting genuine tools or by supplying compromised ones in their place. OSCE MC Decision No. 3/18 commits States to refraining from arbitrary or unlawful interference with journalists' use of encryption and anonymity technologies.[62] The Council of Europe equally requires a legal framework safeguarding the confidentiality and security of communications of journalists,[63] and several UN documents highlight the importance of encryption for freedom of expression.[64] A useful indicator of a State's commitment to privacy and cybersecurity is therefore not only whether it protects the use of encryption and anonymity technologies relied

61 Committee to Protect Journalists (26 June 2026) Russian independent journalists fear MAX app, new online restrictions will hinder reporting. Available at https://cpj.org/2026/06/russian-independent-journalists-fear-max-app-new-online-restrictions-will-hinder-reporting/ [Accessed 27 July 2026] ; Reporters Without Borders (27 November 2025) In Ukraine's occupied territories, the Kremlin's messaging app Max is building a digital Iron Curtain. Available at https://rsf.org/en/ukraine-s-occupied-territories-kremlin-s-messaging-app-max-building-digital-iron-curtain [Accessed 27 July 2026].

62 OSCE (2018) Ministerial Council Decision No. 3/18 on the Safety of Journalists. Vienna: OSCE.

63 For example, CM/Rec(2016)4 on the protection of journalism and safety of journalists and other media actors, and case law by the European Court of Human Rights, such as Standard Verlagsgesellschaft mbH v. Austria (no. 3).

64 For example, UNESCO (2016), Human rights and encryption, https://www.unesco.org/en/articles/human-rights-and-encryption [Accessed 26 August 2026] or reports by the UN Special Rapporteur on Freedom of Expression such as A/HRC/23/40 or A/HRC/29/32.

upon by journalists, human rights defenders, civil society and other high-risk users, but whether the infrastructure it makes available for that purpose is genuinely independent of the State's own reach.

Increased protection would require States to encourage adoption and interoperability of high-risk-user device protections with independent forensic investigators, while ensuring such voluntary technical measures do not substitute for binding legal safeguards. In this context, supporting and resourcing independent forensic detection capacity (such as Amnesty International's MVT) and the labs that operate them can facilitate identification and evidencing of compromise. Overall, State support for journalists' digital skills and strengthened cyber-resilience can increase protections and effectiveness of existing safeguards, as also highlighted in the European Commission's Recommendation on the protection, safety and empowerment of journalists.

CONCLUSION

This brief opened by asking whether the existing architecture of protection, built around interception warrants, is still calibrated to the scale and covertness of contemporary surveillance, including spyware, biometric identification and AI-assisted analytics. The answer developed across the preceding sections is that the architecture does not need to be discarded, but it does need to be discarded, but it does need to be reinterpreted. Existing frameworks and commitments, from the ICCPR and ECHR to OSCE MC Decision No. 3/18 and EMFA, remain conceptually sound: authorization, oversight, notification and remedy remain the right instruments. What has shifted is the

point at which interference with journalistic functions and sources now occurs. These instruments were designed around a discrete act of collection, be it interception, a source-disclosure order or a device seizure, that an authorizing body could authorize in advance and an oversight body could review after the fact. RFoM Communiqué No. 1/2023 already recognized that certain tools sit outside what this architecture can accommodate; the Representative's April 2026 report to the Permanent Council goes further, warning that technological change is outpacing the safeguards meant to contain it. A framework built to review collection has little purchase where a source is identified not through interception but through aggregation and analysis of data already lawfully held.

Realizing OSCE commitments in this environment requires extending authorization, oversight, notification and remedy to that analytical layer as directly as they apply to collection, treating identification through inference as no less a surveillance event than identification through interception. This reinterpretation is only as effective as the institutions that carry it out: a judicial authorization requirement reads identically whether the authorizing body is genuinely independent or not; its capacity to constrain the State does not. Protecting journalists and media freedom from undue surveillance, as AI-assisted and biometric capabilities continue to expand, depends on both fronts holding at once: legal thresholds that keep pace with the technology, and the institutional independence needed to make those thresholds mean something in practice. At the same time, it needs to be embedded in strong rule of law systems because genuine checks and balances as well as due process are essential preconditions for protective frameworks to work in practice. Alongside legal, technological, and institutional safeguards, psy-

chological and professional safeguards can also prove essential to better protective frameworks.

OSCE participating States committed themselves in 2018, under OSCE MC Decision No. 3/18, to refrain from arbitrary or unlawful interference with journalists' communications, encryption and anonymity. Honoring that commitment today means applying it to forms of surveillance its drafters could not have anticipated. Safeguarding journalists against emerging surveillance capabilities is consequently a dual undertaking: updating the substantive threshold to match technical reality, and reinforcing the institutional independence that gives any threshold the power to actually constrain the State. The OSCE RFoM offers ten action points for States to better operationalize their commitment to refrain from arbitrary or unlawful surveillance.

ACTION POINTS

10 ACTION POINTS
AND MEASURES ON OPERATIONALIZATION

1. **PRESERVE privacy, online anonymity and secure communications infrastructures to safeguard freedom of expression and media freedom**
    a. Recognize and protect privacy as essential to freedom of expression, media freedom, and, more broadly, human rights and democracy. Assess privacy implications and journalistic-source-protection risks across all policy areas, including in debates and proposals on identity verification, age assurance and provenance systems which can expose journalistic sources and communications, and account for the heightened and intersectional privacy and surveillance risks faced by journalists, particularly those from marginalized and vulnerable groups in society, and the impact on their ability to work freely and protect confidential sources.
    b. Acknowledge that encryption and anonymity technologies are essential safeguards for secure communications and important for protecting freedom of expression online; do not unduly restrict the development, distribution, or use of these technologies, and do not treat the use of anonymity tools, end-to-end encrypted communication platforms, or VPNs as stand-alone or prima facie evidence of wrongdoing; and do not mandate or knowingly maintain backdoors in encryption or other deliberate cybersecurity vulnerabilities.
    c. Refrain from mandating or promoting communications infrastructure that enables surveillance by design, intercepts mass communication, centralizes excessive data collection and/or retention without oversight, or displaces secure and independent alternatives.

2. **PREVENT undue surveillance through a robust legal framework**
   a. Establish or strengthen comprehensive legal frameworks governing surveillance, in line with international human rights law, through inclusive and transparent legislative processes involving civil society and other relevant stakeholders. Where a measure risks interfering with journalistic functions, exposing journalistic sources, or otherwise affecting media freedom, whether intentional or unintended, and as soon as knowledge of such risk is gained, mandate additional procedural safeguards and documented justifications.
   b. Refrain from arbitrary or unlawful surveillance of journalists (in line with OSCE Ministerial Council Decision No. 3/18). Conduct surveillance as an exception and not the rule, only on the basis of due process and where justified under the three-part test of the cumulative criteria of legality, legitimacy, and necessity and proportionality, together with non-discrimination and adequate procedural safeguards.
      - **Legality**
        Require a clear, accessible, and foreseeable legal basis for any surveillance measure – the collection or interception of data, regardless of the technologies and capabilities used – rather than only for specific tools. Ensure this covers not only direct interception but also indirect surveillance (e.g. through metadata, AI-assisted inference, aggregation and analysis) as soon as knowledge of such indirect surveillance is gained, measures that in combination produce surveillance effects, and non-digital methods such as compelling disclosure of passcodes or biometric device unlocking, search and seizure of equipment, as

well as biometric identification (facial recognition, gait analysis, voice-print matching). Ensure that buying, analyzing, or otherwise using commercially available datasets, or outsourcing surveillance, cannot circumvent protective frameworks or evade safeguards.

- **Legitimacy**
  Permit surveillance only where demonstrably and exclusively justified by a legitimate aim recognized as permissible grounds for restricting the right to privacy and freedom of expression in international human rights law. Do not treat technical capability or convenience as a legitimate aim. Do not invoke "national security" or "public order" grounds as a pretext for restricting freedom of expression; any such invocation must be exceptional, strictly necessary and proportionate, evidence-based, and subject to independent oversight.
- **Necessity and proportionality**
  Require a documented necessity and proportionality assessment before authorizing any surveillance measure, setting its duration or renewing it, with decisions subject to independent oversight and regular review. Assess proportionality ex ante against the comprehensive impact of a measure and the specific capabilities of the employed technology. Request the authorizing authority to demonstrate the exhaustion or inadequacy of other investigative means; use surveillance as last resort.

c. Identify surveillance capabilities, tools and technologies that are by design and a priori disproportionate due to their pervasive and indiscriminate nature, in particular where they provide unrestricted, real-time access to personal data, microphones, and cameras, and prohibit their development, use, production, sale, import, and export. Carefully consider whether the use of spyware is in principle reconcilable with the right to privacy and freedom of expression, keeping in mind that it seems "very hard to imagine that the use of extremely pervasive and intrusive spyware on journalists and other media actors can ever be considered compatible with the principles agreed upon in the OSCE", as stated in the OSCE RFoM Communiqué No. 1/2023.
d. If derogations are invoked in line with the respective provisions of the international human rights instruments in times of emergency or conflict, ensure that such derogations are limited to what is strictly required by the exigencies of the situation.

3. PRIORITIZE independent, individualized, narrowly scoped authorization

a. Vest authorization powers in an independent, preferably judicial, authority with technical expertise (or advice) and capacity as well as knowledge of international human rights standards. Ensure institutional and operational conditions necessary to safeguard its independence and impartiality. Require the authorizing body to consider the combination of measures and analysis, and to assess and protect against cumulative surveillance risks, source exposure, gendered targeting, legal harassment, and transnational reach.

b. Require prior, individualized authorization tied to a specific purpose, a targeted and time-bound intervention, and a defined data focus, grounded in data minimization, retention limits, and mandatory deletion timelines. Document each authorization. Do not permit open-ended authorizations; require separate authorization for each stage and for secondary use or sharing for purposes beyond the original authorization, e.g. authorizing interception of a journalist's communication does not authorize the use of algorithms to infer their source network from the resulting metadata. Require authorization to protect the integrity of digital evidence, ensuring surveillance powers are not used to plant, manipulate, or delete data on a target device, or to generate or alter AI-assisted inferences.
c. Where authorization is not possible before collection in exceptional and urgent circumstances expressly prescribed by law, require it before any analysis of the data, within a short, legally defined timeframe.

4. PERFORM independent oversight

a. Ensure oversight is conducted by an independent judicial or equivalently competent independent authority, and guarantee the independence of the oversight body in law and in practice, based on genuine separation of powers and rule of law. Consider the establishment of a dedicated surveillance watchdog or ombudsperson.
b. Provide continuous or contemporaneous oversight, proportionate to the intrusiveness and risk of the measure, in addition to ex post oversight. Extend oversight to the full data lifecycle of surveillance measures: collection, analysis, storage, sharing, and deletion. Equip the oversight body with the technical

expertise, capacity, and resources to audit systems, including AI-assisted analytical tools, audit logs and data-access traces. Require persistent, tamper-evident audit logs of every query and inference, to enable oversight.

c. Provide oversight bodies with corrective and interim powers (e.g. compelling the cancellation of data collection or analysis mid-surveillance if an authorization is exceeded), distinct from individual remedies, and with the power to act on their own initiative.
d. Strengthen existing regional and multilateral human rights structures to establish dedicated surveillance monitoring and reporting mechanisms, and to include surveillance oversight, where feasible, particularly to address transnational repression or captured institutions.

5. **PROVIDE accountability and redress through notifications, investigations, and remedies**
   a. Mandate notification for any surveillance measure within a short, legally defined timeframe, once notification no longer seriously jeopardizes the legitimate purpose of the measure, with access to relevant data documentation; also notify incidentally affected third parties. Require additional justifications and authorization before notifications can be delayed on grounds of exceptional and urgent circumstances.
   b. Provide meaningful complaint mechanisms where there are reasonable grounds to suspect surveillance, irrespective of a notification, and ensure impartial and effective investigations of unlawful surveillance, including when unlawful interception of personal data is committed by non-State actors, with dedicated protocols for transnational repression and protection of exiled journalists; ensure that in every case of the unlawful

surveillance of a journalist, regardless of whether it is committed by a State agent or a private actor, the potential link between the unlawful surveillance and its target's journalistic activity is properly investigated. Preserve forensic evidence and documentation for accountability purposes.

c. Ensure access to effective judicial remedies, including compensation, deletion of unlawfully collected or inferred data, and correction of resulting inferences; ensure that redress for undue surveillance draws on the five forms of reparation defined by the UN Basic Principles and Guidelines on the Right to a Remedy and Reparation (restitution, compensation, rehabilitation, satisfaction, and guarantees of non-repetition).
d. Beyond legal remedies and forensic support, consider providing legal aid, psychosocial support, and rapid-response victim assistance. Provide dedicated support for exiled journalists, including through forensic agencies, regardless of nationality or immigration status.
e. Establish accountability frameworks setting out the responsibilities of vendors and the private sector, including a duty to conduct human rights due diligence and verify that authorizations and assessments are in place throughout the surveillance lifecycle. Criminalize unlawful surveillance in cases of deliberate or reckless abuse and provide administrative sanctions for technical non-compliance; ensure traceability and attribution at every step of the authorization process to hold State officials individually accountable; ensure that criminal liability is extended to serious cases of unlawful intrusion into a journalist's private life committed by non-State actors.

6. PUBLISH information and guarantee transparency

a. Make legal frameworks and permissible grounds for surveillance public, even where operations remain secret, and disclose which tools, programs, and technologies are available (including those developed in-house), while managing cybersecurity risks.
b. Publish strategies and annual reports on surveillance use, while managing the risks of revealing sensitive data, and periodically assess and report on law enforcement practices and evolving surveillance technologies, with specific attention to vulnerable groups, exiled journalists, and women journalists.
c. Mandate transparency for companies developing surveillance tools to ensure accountability, including on ownership, internal human rights policies, due diligence processes, and remedial action, where applicable.

7. PROCURE and invest in accordance with human rights

a. Suspend acquisition of any surveillance tool where human rights-compliant development or deployment cannot be ensured. Procure only from accountable partners; reduce dependence on opaque commercial vendors whose incentives and governance cannot be controlled; do not share excessive data with them; and maintain a public registry and blocklists.
b. Require ex ante and ex post human rights due diligence for any investment in technologies with surveillance capabilities.
c. Make sure that in-house development (if a State builds its own monitoring, tracking, or data-collection soft- or hardware) does not circumvent transparency and human rights due diligence.

8. PROTECT journalists and their sources across borders through export control

a. Require human rights due diligence before exporting or granting a license, including assessment of destination risks (and compounded impacts), end-user verification, and prohibited end uses; issue licenses only for a limited period. Maintain end-use monitoring and compliance throughout licensing periods; review and revoke licenses where necessary, and investigate credible misuse or newly emerging information.

b. Document and publish aggregated licensing data as well as the impact assessment and the reasoning for approvals and refusal. Provide for export restrictions and company blocklists, and maintain a public registry.

c. Consider enabling accountability mechanisms for the exporting State if due diligence requirements are not respected; ensure a person targeted abroad with a capability exported, brokered or licensed under the State's jurisdiction can bring a claim before its courts or an equivalent independent body, irrespective of nationality, residence or the place where the harm occurred.

9. PRECLUDE proliferation through market regulation

a. Recognize the risk of commercial cyber-intrusion market proliferation for human rights, media freedom, and cybersecurity, and consider imposing a moratorium on the sale or use of such surveillance technologies.

b. Regulate private-sector surveillance, including by protecting against purpose-built and functionally equivalent extraction tools, as well as by banning technologies that are incompatible with human rights. Address through human rights-based regulation the im-

pact of private, non-State actors on the safety of journalists, including through smart home devices, drones, smart glasses, or geotagging or ad-tech location data.

c. Consistently require implementation of companies' own human rights responsibilities under the UN Guiding Principles on Business and Human Rights.

10. PROMOTE human rights through multi-stakeholder partnerships and support

a. Foster multi-stakeholder dialogue and international co-operation, including through cross-border investigations, international registries of authorized vendors and blocklists, and human rights sanctions.

b. Support digital security ecosystems, secure-by-default technology, co-ordinated disclosure of existing vulnerabilities, and independent threat-notification services; support initiatives aimed at identifying and evidencing compromise and mitigating harm after detected compromise, including voluntary technical measures, device protections, and independent forensic investigators and detection capacity. Provide opt-in protective and detection support specifically for exiled journalists.

c. Cooperate with civil society, journalists' associations, the digital security sector and the media, including employers, providing support, training, and funding; recognize civil society as a partner in preventing undue surveillance affecting media freedom and mitigating its impact, as a credible forensic source, an enabler of remedy, and supporter of oversight mechanisms. Build and strengthen national safety of journalists' structures, including by adopting national action plans, and build on and streng-

then existing digital safety and security initiatives and networks. Engage continuously with civil society, academia and other stakeholders to identify and assess risks, provide oversight, and foster accountability.

d. Connect these efforts to broader media freedom challenges, such as online violence or Strategic Lawsuits Against Public Participation (SLAPPs), often interlinked with surveillance, and thus address the whole ecosystem of attacks against journalists and media freedom.


osce
the representative
on freedom
of the media